Enclosure 2

RG&E GINNA STATION PRESENTATION TO NRC

SEPTEMBER 24, 2002

Ginna License Amendment Request
CREATS Actuation Instrumentation LCO 3.3.6

PURPOSE OF BRIEFING

- Provide NRC with an overview of the proposed responses to the 36 NRC questions dated Aug 28, 2002
- Provide NRC with an overview of the Inovision V&V Program for the Model 956
- Review schedule

NRC QUESTION RESPONSES

- For each of the 36 NRC questions from the August 28th letter, proposed responses have been developed along with the attachments requested or needed to provide more detail. An overview of the answers and description of the associated attachments is included here. The purpose is to gain NRC feedback on the level of detail and ensure the necessary documentation responds to the question.

BACKGROUND

- Pre-1984 - Single radiation monitor (R-1) in the control room
- 1984 - Installed 3 diverse radiation monitors (R-36, R-37, and R-38) which take a suction from the control room ventilation system intake and provide input to a single train of actuation logic

BACKGROUND

- The current system has had a number of failures and issues associated with it
  - component failures
  - electronic noise
  - replacement part quality concerns
  - obsolescence of replacement parts

BACKGROUND

- Replace existing actuation instrumentation system with 2 redundant radiation monitors placed directly within the control room ventilation system intake
- Configure radiation monitors and actuation logic into 2 redundant trains, including 2 manual actuation switches

QUESTION 36

- Large LOCA is the accident analyzed in Ginna UFSAR Section 6.4, "Habitability Systems"
- FHA has higher source term, but shorter duration, so initiation setpoint is acceptable
- Remaining accidents have no specific Control Room dose analysis available. Instead, qualitative reviews of offsite doses were reviewed/performed.
  - Rod ejection/SBLOCA - 10% fuel failure results in rapid system response
  - SGTR and MSLB - qualitative review using X/Q ratio shows < GDC 19 without isolation

QUESTION 36 (Cont.)

– Tornado Missile - plant procedures require placing ventilation system in recirculation for a tornado watch

QUESTION 1

- Inovision Model 956A unit has been qualified for EMI/RFI in accordance with EPRI TR-102323 Rev. 1 as documented in Attachment 1.
- Testing performed by F-Squared Lab in Ohio.
- Exceptions to range or testing in TR Rev. 1 under evaluation per TR Rev. 2
- For any exceptions to Rev. 2, testing will be re-performed by Nov. 1, 2002.

QUESTION 2

- RG&E FMEA Performed for CREATS Instrumentation System
- To be provided to NRC as Attachment 2.

QUESTION 3

- EE-171 is to be provided to NRC as Attachment 3.
- C of C to RG&E to be provided as Attachment 4.
- NUPIC audit of Inovision to be provided as Attachment 5.

QUESTION 4

- 4.A) Same hardware and software design for 94X and 956A. Difference is in the process application:
  - 942 – Process instrument
  - 946 – Ion Chamber
  - 956A – G-M Tube
  - Software for each is configured for the application

QUESTION 4 (Cont.)

- 4.B) Model 94X and 956A design and testing, per the Victoreen QA Manual was done in the 1980's.
  - Since then Victoreen (now Syncor) has been audited by NUPIC and approved.
  - Now, Syncor is performing a V&V Program following EPRI TR-103291 Rev. 1 (addressed in detail in a later question)

QUESTION 4 (Cont.)

- 4.C) Over 200 Model 956A's in service throughout the U.S. and world in nuclear and non-nuclear applications. Attachment 6 will be provided to the NRC documenting the listing of locations for use.

QUESTION 5

- There has never been a reported failure in the nuclear OE database.
- The vendor noted that replacement parts are ordered by clients. All customer noted interactions as related to model 956 have been non-failure mode maintenance.

QUESTION 6

- 6.A) Memory chips are not the same as timing and system interface and are CMOS type devices
- 6.B) Chips are soldered in place and are qualified as documented in Syncor Qualification Report 950.366 included.

QUESTION 6 (Cont.)

- 6.C) The memory organization is very simple – intended to perform only the very limited functions required for each model application. It is not a complex program with multi-functions or tasks running at the same time.

QUESTION 7

- 7.A) The assembled code was compared through functional testing such that the differences are considered minor.
- 7.B) HP64100 and American Arium Development System were commercially available software development tools, when the software was developed.
  - Firmware was subjected to the factory acceptance testing for Appendix B qualification

QUESTION 8

- Software V&V Plan
- The V&V will be forwarded to the NRC as Attachment 7 and includes:
  - Software Requirements Specification (SRS)
    - Software requirements specifications
  - Software Design Description (SDS)
    - Software description, software flow diagram, interrupts, watchdogs
  - Software V&V Test Procedure
  - Software V&V Test Report
  - Software V&V Matrix
  - Software Design Reviews

V&V PLAN OUTLINE

1 Purpose

2 Referenced Documents

3 Definitions

4 Verification and Validation Overview

5 Life-Cycle Verification and Validation

6 Software Verification and Validation Reporting

7 Verification and Validation Administrative Procedures

SRS OUTLINE

SDD OUTLINE

1 Introduction
1.1 Purpose
1.2 Scope
1.3 Definitions and Acronyms

2 References

3 Decomposition Description
3.1 Module Decomposition
3.2 Concurrent Process Description
3.3 Data Decomposition

4 Dependency Description
5 Interface Description
5.1 Module Interface
5.2 Process Interface

6 Detailed Design
6.1 Module Detailed Design

QUESTION 9

- Model 956 completed design and QA testing in 1985.
- Since then over 200 model 956 units have been installed and operated over 3 million hours
- Originally designed and tested per 10 CFR 50 App. B
- Software V&V per EPRI TR-103291

QUESTION 10

- Earlier qualification program documents being provided to NRC as Attachment 8.
- Attachment 9 will provide:
  - Current vendor test plan and procedures
  - System manual
  - Operator instruction manual
  - Written factory acceptance test procedure
- Attachment 10 will provide RG&E review of factory acceptance testing.

QUESTION 11

- As requested, vendor manual will be provided in Attachment 10.9
- Attachment 11 will provide RG&E procedures:
  - IP-DES-2
  - IP-DES-4

QUESTION 12

- Syncor has a NUPIC audited design control program that documents by Engineering Change Notice upgrades for both hardware and software. QSP-205 is the control procedure in QA Manual.
- Syncor QA Manual will be provided as Attachment 12.
- EPROM controlled by Revision level.
- RG&E currently does not have equipment to perform upgrades at this time.

QUESTION 13

- From IEEE Std 603 Review Document Section 4.9
  - "The appropriate reliability level requirements for this safety function have been determined by reviewing the operating requirements and comparing them to the criticality of operation of the safety function with respect to time and consequences." Factors considered in qualitatively evaluating reliability were redundancy of components, independence of the redundant trains, fail-safe operation of safety function actuating components, and cross-train connection of isolation signals to minimize the possibility of an actuating signal from being prevented. All of these factors have been incorporated into the design to maximize the reliability of the safety system, consistent with the criticality of the performance of this safety system.

QUESTION 14

- The Ginna CREATS Instrumentation PSA is to be included as Attachment 13.
- Common cause failures (CCFs) were determined using beta factor method
  - Used device with highest failure probability (radiation element)
  - Assumed beta factor of 2.5% (per NUREG/CR-5485)
  - CCFs account for 76% of calculated results

QUESTION 15

- Syncor documents to be included in Attachment 9.

QUESTION 16

- A copy of the latest NUPIC audit with two findings is included in Attachment 5. The statement on non-conformances means that no non-conformances were received by Syncor for the model 956.
- Users are not required to report non-conformances but are encouraged to report operation or performance issues that affect customer satisfaction.

QUESTION 17

- No specific evaluation of software common mode failure was performed.
- V&V process and quality control will provide reasonable assurance that likelihood of software failure is sufficiently low.

QUESTION 18

- Yes – see section 4.8 of the referenced response
  - The equipment has been specified, designed, and installed in a configuration and in locations that will not result in the degradation of safety system performance for any conditions described in the UFSAR for the applicable design basis events listed in section 4.1. All appropriate design provisions have been incorporated to retain the capability for performing the safety functions required for those events. Other events, (such as fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in a non-safety system, or missiles and pipe breaks not listed in section 4.1), either do not degrade the system or do not result in a condition that will require the system to perform its safety function.

QUESTION 19

- Isolators purchased as safety related from an Appendix B vendor (Sciencetech/NUS) and perform the isolation function as specified in IEEE 384-1981.

QUESTION 20

- Fuses provide isolation of 120VAC control circuits only and are not relied upon for signal isolation.

QUESTION 21

- The Syncor Product Information Bulletin is being provided as Attachment 14 which is a summary of the product history.

QUESTION 22

- Attachment 15 contains a listing of all components including those purchased as safety related including:
  - Radiation monitors (detector and ratemeters)
  - Control board components
  - Control relays
  - Terminal blocks

QUESTION 23

- RG&E document EE-100 is included as Attachment 16.

QUESTION 24

- RG&E Nuclear Assessment Procedure QA-PES-1 is included as Attachment 17.

QUESTION 25

- 25.A) The safety function of the computer is to read data, determine when the setpoint is reached, and change the output state of a contact to initiate CREATS isolation.
- 25.B) Characteristics are identified in the SRS, SDD, Matrix and V&V Test Procedure (Attachment 7)
- 25.C) Demonstrated by V&V Test Procedure and documented in V&V report.

QUESTION 26

- Qualification Report included as Attachment 1 – documents temperature and humidity range.
- Environmental requirements bound those specified in the Ginna UFSAR for those accidents which CREATS instrumentation is required to operate.

QUESTION 27

- Attachment 1 has a copy of the IRM Qualification Test Report and Data (Qual. Report 950.366.)

QUESTION 28

- Diagnostic coverage for computer functions will be identified in the SRS and SDD to be provided to NRC with the V&V Report.

QUESTION 29

- The RG&E test plans are contained in the Test Instructions contained in Attachment 18.

QUESTION 30

- Backup provided in the non-safety related area radiation monitor, R-1, in the control room. This monitor (model 946) also provides an alarm and partial control room isolation.
- Also, the Ginna Nuclear Emergency Response Plan provides for on-shift radiation protection technician support which includes control room monitoring.

QUESTION 31

- Review to IEEE 384 provided in RG&E design analysis DA-EE-2001-009, Section 5.6 being provided to the NRC as Attachment 19.

QUESTION 32

- Similar to Question 16.
- A copy of the latest NUPIC audit with two findings is included in Attachment 5.
- Users are not required to report non-conformances but are encouraged to report operation or performance issues that affect customer satisfaction.

QUESTION 33

- Required system response time described in RG&E Engineering Analysis DA-EE-2001-013 (previously submitted).
- Response time testing of CREATS is currently verified using end-to-end testing that confirms UFSAR assumptions during required TS tests.

QUESTION 34

- Monitors calibrated per RG&E Procedure CPI-MON-R45 and CPI-MON-R46.
- Data sheets with as-found values, required values, and allowable tolerances defined
- Out-of-tolerance values addressed immediately by corrective action process per RG&E Procedure IP-CAP-1.

QUESTION 35

- RG&E setpoint program updated in the past three years per ISA-S67.04-1994 Part I and II.
- Calculations performed to 95/95 per the ISA Standard and NRC Regulatory Guide 1.105 Rev. 2.
- Drift analysis provided for all Tech. Spec. calculations

SCHEDULE

- Submit by October 4, responses to questions:
  - 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 29, 30, 31, 32, 33, 34, 35, 36
- Submit by November 1, responses to questions:
  - 1, 8, 9, 25, 28,

SOFTWARE VERIFICATION AND VALIDATION PLAN
FOR
PROM P/N 94095603
GM- AREA MONITOR

REV. LEVEL	ECN #	DESCRIPTION/PAGES AFFECTED

ENGINEERING	DATE 9-20-02
MANUFACTURING	DATE 9/20/02
QUALITY ASSURANCE	DATE 9/20/02

SYNCOR RADIATION MANAGEMENT	DATE 9/11/02	TITLE SOFTWARE VERIFICATION AND VALIDATION PLAN, 94095603				
REV	ECN NO.	RELEASED FOR PRODUCTION	DOC CTRL	SHEET	NO.	SIZE
1	3044			1 of 27	94095603VVP	

Table of Contents

PURPOSE

The purpose of this Verification and Validation plan is to develop a series of activities, and their associated inputs and outputs, that will demonstrate that the firmware in the P/N 94095603 EPROM, used in the Victoreen Model 956A Digital G-M Area Monitor Readout, manufactured by Syncor Radiation Measurements meets the monitor's design requirements and exhibits a high degree of reliability.
Note that although the base firmware was developed in the early 1980s, prior to the availability of the current industry software development standards, this V&V plan is intended to demonstrate that the existing firmware is suitable for use in safety related applications.

1 REFERENCE DOCUMENTS

The reference standards used for guiding the preparation of this document and for SV&V implementation are listed below:

1.1 IEEE Std 7-4.3.2-1993, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

1.2 IEEE Std 610.12-1990, Glossary of Software Engineering Terminology

1.3 IEEE Std 729-1983, Standard Glossary of Software Engineering Terminology

1.4 IEEE Std 829-1991, Standards for Software Test Documentation

1.5 IEEE Std 830-1993, Recommended Practice for Software Requirements Specifications

1.6 IEEE Std 1012-1996, Standard for Software Verification and Validation Plans

1.7 IEEE Std 1016-1987, Recommended Practice for Software Design Descriptions

1.8 IEEE Std 1074-1991, Standard for Developing Software Life Cycle Processes

1.9 EPRI Std TR-103291-CD Handbook for Verification and Validation of Digital Systems (12/1998)

1.10 EPRI Std TR-102348, Rev. 1, Guidelines on Licensing Digital Upgrade

1.11 Syncor Radiation Management Quality Assurance Manual, QSP-100, Version 004, Rev. 1/2/02, Implemented 3/14/02

1.12 Syncor Radiation Management Quality Procedure QSP-205, Document Control

1.13 Syncor Radiation Management Quality Procedure QSP-05-05, Engineering Change Notice

2.11 10CFR50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Jan. 20, 1975

2.12 ANSI/ASME NQA1-1994, Quality Assurance Program Requirements for Nuclear Facility Applications

2 DEFINITIONS

2.1 Definitions

2.1.1 Acceptance testing – Formal testing conducted to determine whether or not the system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system.

2.1.2 Anomaly – Anything observed in operation of the UDR that deviates from expectations based on previously verified software/firmware products or reference documents.

2.1.3 Development team – Team of qualified engineers in charge of applying software development life cycle.

2.1.4 Developer – Member of the development team.

2.1.5 Firmware – The combination of software and data that reside in read-only memory

2.1.6 Firmware component – Assembly language module (set of functions).

2.1.7 Hardware – Physical equipment used to process, store, or transmit computer programs and data.

2.1.8 Life-cycle phase – Any period of time during software development or operation that may be characterized by a primary type of activity (such as design or testing) that is being conducted. These phases may overlap one another; for V&V purpose, no phase is concluded until its development products are fully verified.

2.1.9 Safety related firmware – Firmware for the RMS safety related equipment.

2.1.10 Software – Computer programs and data pertaining to the operation of a computer system.

2.1.11 Software/firmware testing – The process of testing an integrated hardware and software/firmware system to verify that the system meets its specified requirements.

2.1.12 Software tools – A computer program used in the development, testing, analysis, or maintenance of a program or it's documentation. Examples include CASE software, decompiler, driver, editor, flow charter, monitor, test case generator, or timing analyzer.

2.1.13 Software verification and validation plan – A plan for the conduct of software verification and validation.

2.1.14 SSC – Systems, Structure and Components

2.1.15 Test procedure – Documentation that is part of the test report, specifying a sequence of actions for the execution of a test

2.1.16 Traceability – The degree to which a relationship is established between two or more products of the development process, especially product having a predecessor-successor or master-subordinate relationship to one another; for example the degree to which the requirements and design of a given software component match.

2.1.17 Validation – The process of evaluating software/firmware at the end of the software development process to ensure compliance with software requirements.

2.1.18 Validator – Member of the SV&V team who carries out validation.

2.1.19 Verification – The process of determining whether or not the products of a given phase of the software/firmware development cycle fulfill the requirements established during the previous phase.

2.1.20 Verifier – Member of the project team who carries out verification.

2.2 Abbreviations

ANSI – American National Standards Institute

ASCII - American Standard Code for Information Interchange

DOS – Disk Operating System

ECN – Engineering Change Notice

EPROM – Erasable Programmable Read Only Memory

IEEE – Institute of Electrical and Electronics Engineers

PC – Personal Computer

QA – Quality Assurance

RMS – Radiation Monitoring System

SRM – Syncor Radiation Management

SV&V – Software Verification and Validation

UDR - Universal Digital Ratemeter

VVTP - Verification and Validation Test Plan

VVTR - Verification and Validation Test Report

V&V - Verification and Validation

2.3 Acronyms & Notations

PE - Project Engineer

PM - Project Manager

QE – Quality Engineer

QM - Quality Management

PM - Project Manager

PE - Project Engineer

RE – Reliability Engineer

SE – Software Engineer

SM - Syncor Management

SRM - Syncor Radiation Management

TT – Test Technician

2.4 Documentation Names

SRS - Software Requirements Specification

SDD - Software Design Description

SVVP – Software V&V Plan

VVTP - Verification and Validation Test Plan

VVTR - Verification and Validation Test Report

3 Verification & Validation Overview

The overall objective of the V&V Plan for the 94095603 firmware is to assure the program promotes a quality and highly reliable product through an independent process of technical review and evaluation. Note the firmware does not contain an operating system, and performs specific functions on a cyclic basis. A flow chart of the firmware operation is provided in Addendum 1.

The embedded and operating system software and associated tools are predeveloped, or commonly known as legacy software. Like other predeveloped software, it is important to examine the development history to understand how the software has matured with time into the quality product it is today. When the Prom P/N 94095603 firmware was conceived, there was very little guidance in the way of industry standards to base the software development and design on. Good programming practices were used based on the objective of producing a highly reliable safety system.

As expressed in SRP 0800, Appendix 7.0A, the use of digital I&C systems presents the concern that minor errors in design and implementation can cause them to exhibit unexpected behavior. To minimize this potential problem, the design qualification of digital systems needs to focus on a high quality development process that incorporated disciplined specification and implementation of design requirements. Potential common-mode failures caused by software errors are also a concern. One of the protection means against – common-mode software failures is also accomplished by an emphasis on the quality process.

The Prom P/N software was initially developed approximately 15 years ago, evolving into the present day configuration. Within this time frame the product that matured to incorporate enhancements and facility improved hardware design. The evolutionary process will be evaluated to ensure that the pre-developed (Legacy) software is sufficiently reliable for use in nuclear safety related applications.

3.1 Organization

In order to ensure the program supports high quality and reliability, a process of independent technical reviews and evaluations will be performed. The project will be functionally organized under a Project Engineering Manager. The Project Manager will co-ordinate the V&V activities, schedule formal reviews, and document the results of the V&V reviews. The Project Engineering manager may also serve as a member of the V&V review team. A Quality Assurance Engineer will also participate in design reviews to ensure the overall quality of the project is maintained.

The software testing process was strengthened by designating the responsibility for the validation testing to an independent V&V engineer and technician.

An overall project organizational chart is provided below:

Management
-Organization
-Resources
-Follow-up

Qualification
-Quality Assurance
-Quality Control
-V&V

Project Team

Development
-Concept Phase
-Design Phase
-Manufacturing Phase

The project organization is described below:

Syncor Management (SM)----------Quality Management (QM)
|
|---Project Manager (PM)
|
|---Project Engineer (PE)
|
| --------Independent SV&V Engineer (V&V)
|
|---------V&V Test Support Technician (V&V)
|
|---Quality Engineer (V&V)

The staff members that will participate in the V&V effort are:

Name:	Function	Team	Resource
J. Hale	Systems Business Manager	SM	SM
Zis Giatis	QA Manager	QM	QM
Judy Ellis	Software Engineer	V&V	SE
Andy Lasko	Project Manager	PM	PM
Dave Warner	Reliability Engineer	V&V	RE
Dave Smith	Quality Engineer	V&V	QE
George Buck	Test Technician	V&V	TT

The Project Manager will participate in the V&V reviews, and has the authority to resolve issues raised during the V&V.

3.2 Master Schedule

The V&V project is presently planned for completion on an expedited basis, over a 3-month period. At the end of the process, a formal SV&V report will be issued. Progress will be reported on a periodic basis, typically monthly.

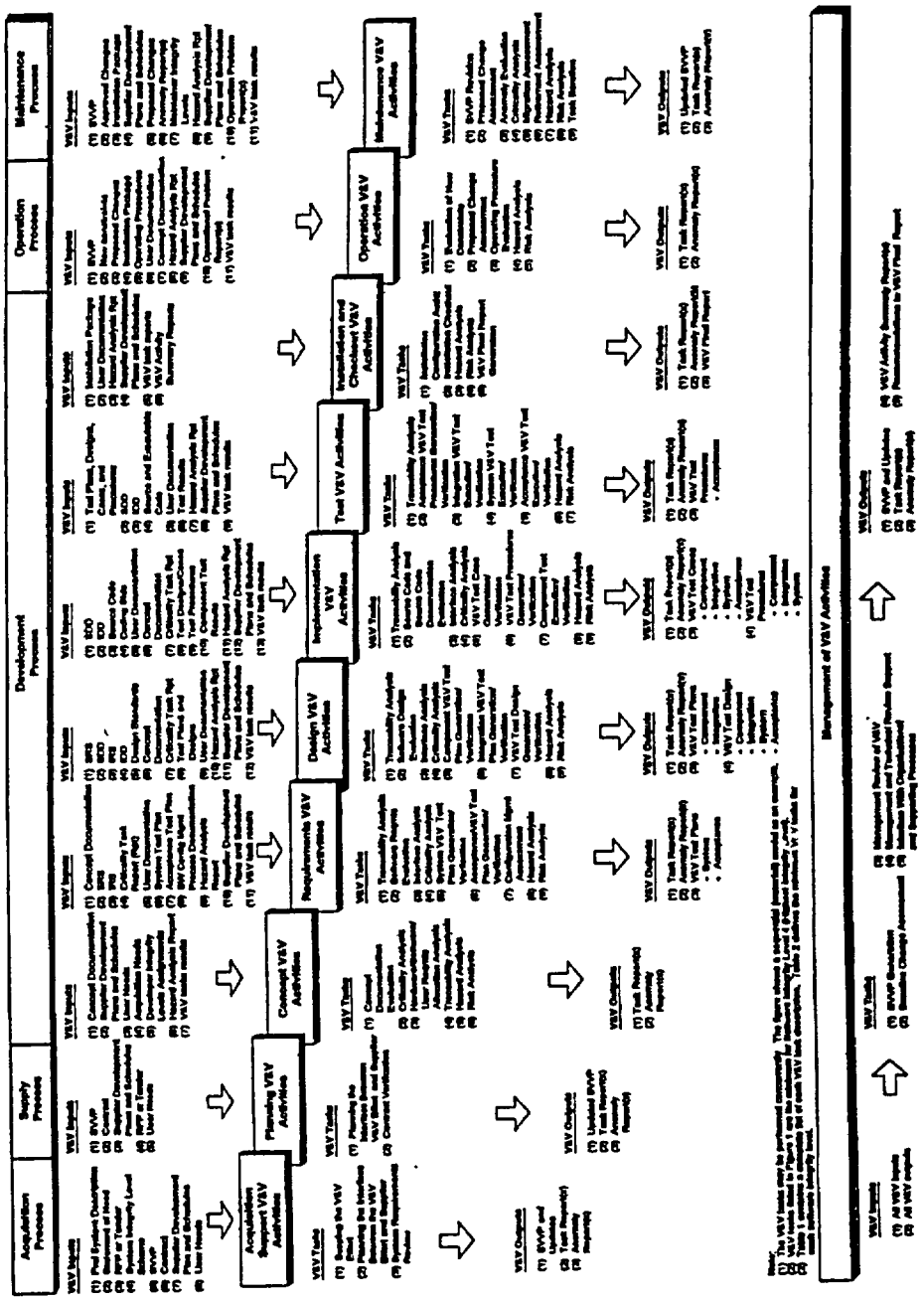
The SVV overview shown below summarizes the life-cycle model used for the project. It is based on the sample model defined in IEEE 1012, except as follows:

-For this project, the design phase has been previously completed, but has not been formally documented. This plan is designed to document the firmware that has been designed. The product is presently in the Maintenance phase.

-Installation, checkout, and operation are performed by the user

Major schedule milestones are listed below:

Complete SRS	Sep. 30, 2002
Complete SDD	Oct. 15, 2002
Complete VVTP	Oct. 30, 2002
Complete VVTR	Nov. 1, 2002



SYNCOR RADIATION MANAGEMENT				DATE 9/11/02	TITLE SOFTWARE VERIFICATION AND VALIDATION PLAN, 94095603	
REV 1	ECN NO. 3044	RELEASED FOR PRODUCTION	DOC CTRL	SHEET 10 of 27	NO. 94095603VVP	SIZE

3.3 Resources Summary

Resources available for this project will include:

3.3.1 Project Manager

3.3.2 Project Engineer

3.3.3 Software/Firmware Engineer

3.3.4 Test Technician

3.3.5 Quality Assurance Engineer

In addition to the above, the following equipment will be required:

3.3.6 1, 956A-201 UDR

3.3.7 1, Signal Generator

3.3.8 1, Digital Voltmeter

3.3.9 1, 94095603 EPROM

3.4 Responsibilities

3.4.1 The SRM Project Manager/Project Engineer is responsible for the implementation of this plan, identifying requirements, resolving problems, and ensuring compliance to the requirements identified by SRM personnel and any subcontractors employed.

3.4.2 The Software Engineer is responsible for reviewing the code, and providing the documents identified in the SV&V Plan. The Software Engineer is also responsible for implementing the V&V tests.

3.4.3 The Test Technician is responsible for assisting the Software Engineer with the V&V tests.

3.4.4 The Quality Assurance Engineer is responsible for reviewing the documents, and ensuring the quality requirements of the SV&V Plan are maintained.

3.5 Tools, Techniques, and Methodologies

The methods used in the V&V process will include review by cognizant engineering personnel, independent verification, and formal reviews.

The tools that will be used for the V&V process are as follows:

Document Preparation:

-Networked PC, Microsoft Word for Windows

-The documentation provided shall be written on a PC using a word processor program; e.g., Microsoft Word or a flat ASCII text editor, or similar. Each page of the document shall have a page header. The page header shall include the document name, part number, revision level and page number.

Target Hardware

-Model 956A-201 UDR with 94095603 EPROM

Test

Signal Generator

Software Testing

-American Arium Assembler/Linker

--DOS Based Personal Computer

For this project, Third Party Software is limited to assembly, emulation, linking and program development tools identified above. The Model 956 firmware is programmed assembly language, and does not include an operating system

4 Life-Cycle Verification and Validation

Outputs from phase tasks are used to develop corresponding V&V phase summary reports and are ongoing inputs to the SVVR. Outputs of V&V tasks become inputs to subsequent life-cycle V&V tasks.

5.1 Management of V&V

4.1.1 V&V Tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Software Verification and Validation Plan (SVVP) Generation. Generate an SVVP for all life cycle processes. The SVVP may require updating throughout the life cycle. Outputs of other activities are inputs to the SVVP.	SVVP (previous update) Contract	SVVP and Updates	PM
Baseline Change Assessment. Evaluate proposed software changes (e.g., anomaly connections and requirement changes) for effects on previously completed V & V tasks. Plan iteration of affected tasks or initiate new tasks to address software baseline changes or iterative development processes. Verify and validate that the change is consistent with system requirements and does not adversely affect requirements directly or indirectly. An adverse effect is a change that could create new system hazards and risks or impact previously resolved hazards and risks.	SVVP Proposed Changes Risks identified by V & V Tasks	Updated SVVP Task Report(s) – Baseline Change Assessment Anomaly Report(s)	PM
Management Review of V & V. Review and summarize the V & V effort to define changes to V & V tasks or to redirect the V & V effort. Recommend whether to proceed to the next set of V & V and development life cycle activities, and provide task reports, anomaly reports, and V&V Activity Summary Reports to the organizations identified in the SVVP. Verify that all V & V tasks comply with task requirements defined in the SVVP.	SVVP and Updates	Updated SVVP Task Report(s)- Recommendations V & V Activity Summary Reports Recommendations to the V&V Final Report	PM, SM, QE

4.1.2 Risks

The risks identified to date are:

4.1.2.1 V&V personnel requires capabilities and attitudes that differ from those encountered during software development.

Impact: A reduction in the motivation of the verifier/validator may have a negative effect on the quality of the product.

Action: Periodically, (each week), a meeting is held between the members of the V&V team and project manager. This meeting promotes teamwork:

- Each member of the V&V team to report work progress, to express any technical and personal communication problems encountered.

-Anticipation of events before they occur thus avoiding technical and motivational problems.

4.1.2.2 The projection of the workload involved in the V&V tasks may be incorrect (over- or underestimated, workload not well distributed).

Impact: adverse effect on schedule

Action: The periodic monitoring (monthly) perceives these shortcomings and defines corrective actions.

4.2 **Acquisition Support** (Acquisition Process) - Not Required; Customer inputs are specified in purchase documents, and customer review/approval of SVVP, SRS, and SDD will be obtained.

4.3 **Planning** (Supply Process) - Not Required; See 5.2 above

4.4 Development Process

4.4.1 Concept Phase of V&V

4.4.1.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Concept Documentation Evaluation. Verify that the concept documentation satisfies user needs and is consistent with acquisition needs. Identify major constraints of interfacing systems and constraints or limitations of proposed approach. Assess criticality of each software item.	Concept Documentation User Needs Acquisition Needs	Task Report- Concept Documentation Evaluation Anomaly Report(s)	PM, QE, SM, SE

4.4.1.2 Risks

4.4.1.2.1 Product performance may not fully envelope customer requirements.

Impact: Be aware that initial performances may fall short of meeting all customer expectations.

Action: Anomalies will be identified and reviewed with the customer for ultimate disposition.

4.4.2 Requirements Phase of V&V

4.4.2.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Traceability Analysis. Trace the software requirements (SRS) to system requirements (Concept Documentation) and system requirements. Analyze identified relationships for correctness, consistency, completeness, and accuracy.	Concept Documentation SRS	Task Report- Traceability Analysis Anomaly Report(s)	PM, QE, SM, SE
Software Requirements Evaluation. Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS for correctness, consistency, completeness, accuracy, readability, and testability.	Concept Documentation SRS	Task Report(s)-Software Requirements Evaluation Anomaly Report(s)	PM, QE, SM, SE
Interface Analysis. Verify and validate that the requirements for software interfaces with hardware, user, operator, and other systems are connected, consistent, complete, accurate, and testable	Concept Documentation SRS	Task Report(s) - Interface Analysis Anomaly Report(s)	PM, QE, SM, SE
Criticality Analysis. Review and update any existing criticality analysis results from the prior Criticality Task Report using the SRS.	Task Report(s) – Criticality SRS	Task Report(s) – Criticality SRS	PM, QE, SM, SE
System V & V Test Plan Generation and Verification. *(For Software Integrity Levels 1 and 2)* Verify that developer's System Test Plans conform to Project defined test document purpose, format, and content (eg., see IEEE Std 829-1991). Validate that the System Test Plan satisfies the following criteria 1) test coverage of system requirements; 2) appropriateness of test methods and standards used; 3) conformance to expected results; 4) feasibility of system qualification testing; and 5) capability to be operated and maintained.	Concept Documentation (System requirements) SRS User Documentation System Test Plan	Anomaly Report(s) System V&V Test Plan	PM, QE, SM, SE

4.4.2.2 Risks Not applicable

4.4.3 Design Phase of V&V

4.4.3.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Traceability Analysis. Trace design elements (SDD), to requirements (SRS), and requirements to design elements. Analyze relationships for correctness, consistency, and completeness..	SRS SDD	Task Report(s)- Traceability Analysis Anomaly Report(s)	PM, QE, SM, SE
Software Design Evaluation. Evaluate the design elements (SDD) for correctness, consistency, completeness, accuracy, readability, and testability.	SRS SDD Design Standards (e.g., standards, practices, and conventions)	Task Report(s)- Software Design Evaluation Anomaly Report(s)	PM, QE, SM, SE
Interface Analysis. Verify and validate that the software design interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability.	Concept Documentation (System requirements) SRS SDD	Task Report(s) – Interface Analysis Anomaly Report(s)	PM, QE, SM, SE
V & V Test Design Generation and Verification. 1) system testing; and 2) acceptance testing. Continue tracing required by the V & V Test Plan. Verify that the V&V Test Designs comply with Project defined test document purpose, format, and content (e.g , see IEEE Std 829-1991). Validate that the V & V Test Designs satisfy the criteria in V&V tasks.	SDD User Documentation Test Plans Test Designs	System V&V Test Design(s) Acceptance V&V Test Design(s) Anomaly Report(s)	PM, QE, SM, SE

4.4.3.2 Risks Not applicable

4.4.4 Implementation Phase of V & V

4.4.4.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

The code will be reviewed for conventional indenting formatting. File headers, which includes the file name, the author, a description/purpose, definition of variables, sub-routines called, and the modification history, will be used for module modifications.

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Traceability Analysis. Trace the source code components to corresponding design specifications(s), and design specification(s) to source code components. Analyze identified relationships for correctness, consistency, and completeness.	SDD Source Code	Task Report(s) - Traceability Analysis Anomaly Reports	PM, QE, SM, SE
Source Code and Source Code Documentation Evaluation. Evaluate the source code components (Source documentation) for correctness, consistency, completeness, accuracy, readability, and testability.	Source Code SDD Coding Standards User Documentation	Task Report(s) – Source Code and Source Code Documentation Evaluation Anomaly Report(s)	PM, QE, SM, SE
Interface Analysis. Verify and validate that the software source code interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability.	Concept Documentation SDD Source Code User Documentation	Task Report(s) – Interface Analysis Anomaly Report(s)	PM, QE, SM, SE
V&V Test Case Generation and Verification. Verify that the developer's Test Cases conform to Project defined test document purpose, format, and content. Validate that the developer's Test Cases satisfy the criteria for system and acceptance testing.	SRS SDD User Documentation Test Design Test Cases	System V&V Test Cases Acceptance V&V Test Cases Anomaly Report(s)	PM, QE, SM, SE
V&V Test Procedure Generation and Verification. Verify that the developer's Test Procedures conform to Project defined test document purpose, format, and content. Validate that the developer's Test Procedures satisfy the criteria in V&V tasks for system and acceptance testing.	SRS SDD User Documentation Test Cases Test Procedures	System V&V Test Procedures Anomaly Report(s)	PM, QE, SM, SE
Hazard Analysis. Verify that the implementation and associated data elements correctly implement the critical requirements and introduces no new hazards. Update the hazard analysis.	Source Code SDD Hazard Analysis Report	Task Report(s) - Hazard Analysis Anomaly Report(s)	PM, QE, SM, SE
Risk Analysis. Review and update risk analysis using prior reports. Provide recommendations to eliminate, reduce or mitigate the risks.	Source Code Hazard Analysis Report V&V task results	Task Report(s) – Risk Analysis Anomaly Report(s)	PM, QE, SM, SE

4.4.4.2 Risks Not Applicable

4.4.5 Test Phase of V & V

4.4.5.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Traceability Analysis. Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. For correctness, verify that there is a valid relationship between the V&V Test Plans, Designs, Cases, and Procedures. For completeness, verify that all V&V Test Procedures are traceable to the V&V Test Plans.	V&V Test Plans V&V Test Designs V&V Test Procedures	Task Report(s) – Traceability Analysis Anomaly Report(s)	PM, QE, SM, SE
Acceptance V&V Test Procedure Generation and Verification. Verify that the developer's Acceptance Test Procedures conform to Project defined test document purpose, format, and content.	SDD Source Code User Documentation Acceptance Test Plan Acceptance Test Procedures	Acceptance V&V Test Procedures Anomaly Report(s)	PM, QE, SM, SE, RE
System V&V Test Execution and Verification. Use the developer's system test results to verify that the software satisfies the test acceptance criteria.	Source Code Executable Code User Documentation Acceptance Test Plan Acceptance Test Procedures Acceptance Test Results	Test Report(s) – Test Results Anomaly Report(s)	PM, QE, SM, SE, RE, TT
Hazard Analysis. Verify that the test instrumentation does not introduce new hazards. Update the hazard analysis	Source Code Executable Code Test Results Hazard Analysis Report	Task Report(s) – Hazard Analysis Anomaly Report(s)	PM, QE, SM, SE
Rick Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks	Hazard Analysis Report V&V task results	Task Report(s) – Risk Analysis Anomaly Report(s)	PM, QE, SM, SE

4.4.5.2 Risks Not Applicable

4.4.6 Installation and Checkout Phase of V & V

4.4.6.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Installation Configuration Audit. Verify that all software products required to correctly install and operate the software are present in the installation package. Validate that all site-dependent parameters or conditions to verify supplied values are correct.	Installation Package (e.g.. Source Code, Executable Code, User Documentation, SDD, SRS, Concept Documentation, Installation Procedures, site-specific parameters, Installation Tests, and Configuration Management Data)	Task Report(s) - Installation Configuration Audit Anomaly Report(s)	PM, QE, SM, SE
Installation Checkout. Conduct analyses or tests to verify that the installed software corresponds to the software subjected to V & V. Verify that the software code and databases initialize, execute, and terminate as specified. In the transition from one version of software to the next, the V & V effort shall validate that the software can be removed from the system without affecting the functionality of the remaining system components. The V & V effort shall verify the requirements for continuous operation and service during transition, including user notification	User Documentation Installation Package	Task Report(s) - Installation Checkout Anomaly Report(s)	PM, QE, SM, SE
Hazard Analysis. Verify that the installation procedures and installation environment does not introduce new hazards Update the hazard analysis	Installation Package Hazard Analysis Report	Task Report(s) – Hazard Analysis Anomaly Report(s)	PM, QE, SM, SE
Risk Analysis Review and update risk analysis using prior task reports.	Installation Package Supplier Development Plans and Schedules V&V Task Results	Task Report(s) - Risk Analysis Anomaly Report(s)	PM, QE, SM, SE
V & V Final Report Generation. Summarize in the V & V final report the V&V activities, tasks and results, including Report (s) status and disposition of anomalies .	V & V Activity Summary Report(s)	V&V Final Report	PM, QE, SM, SE

4.4.6.2 Risks Not Applicable

4.5 Operation Phase of V & V

4.5.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
Evaluation of New Constraints. Evaluate new constraints (e.g., operational requirements, platform characteristics, operating environment) on the system or software requirements to verify the applicability of the SVVP. Software changes are maintenance activities (see 5.6.1)	SVVP New constraints	Task Report(s) – Evaluation of New Constraints	PM, QE, SM, SE
Proposed Change Assessment. Assess proposed changes (e.g., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V & V tasks would be iterated.	Proposed Changes Installation Package	Task Report(s)- Proposed Change Assessment	PM, QE, SM, SE
Operating Procedures Evaluation. Verify that the operating procedures are consistent with the user documentation and conform to the system requirements	Operating Procedures User Documentation Concept Documentation	Task Report(s) – Operating Procedures Evaluation Anomaly Report(s)	PM, QE, SM, SE
Hazard Analysis. Verify that the operating procedures and operational environment does not introduce new hazards. Update the hazard analysis.	Operating Procedures Hazard Analysis Report	Task Report(s) - Hazard Analysis Anomaly Report(s)	PM, QE, SM, SE
Risk Analysis Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Installation Package Proposed Changes Hazard Analysis Report Supplier Development Plans and Schedules Operation problem reports V&V task results	Task Report(s) - Risk Analysis Anomaly Report(s)	PM, QE, SM, SE
Installation and Operation. These tasks are assigned to Syncor Radiation Management.	Installation Package, Concept Documentation, SRS, Source Code Listings, Executable Code, User Documentation, SVVP, SVVR	Anomaly Report	PM, QE, SM, SE,, QM

4.5.1.1 Risks Not Applicable

4.6 Maintenance Phase of V & V

4.6.1 V&V tasks, Inputs/Outputs, Resources and Responsibilities

V & V Tasks	Required Inputs	Required Outputs	Resources Responsibilities
SVVP Revision. Revise the SVVP to comply with approved changes.	SVVP Approved Changes Installation Package	Updated SVVP	PM, QE, SM, SE
Proposed Change Assessment. Assess proposed changes (e.g., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V & V tasks would be iterated.	Proposed Changes Installation Package	Task Report(s)- Proposed Change Assessment	PM, QE, SM, SE
Anomaly Evaluation. Evaluate the effect of software operation anomalies.	Anomaly Report(s)	Task Report(s) – Anomaly Reports	PM, QE, SM, SE
Retirement Assessment. For software retirement, assess whether the installation package addresses: software support, impact on existing systems, software archiving, transition to a new software product, and user notification.	Installation Package Approved Changes	Task Report(s) – Retirement Assessment Anomaly Report(s)	PM, QE, SM, SE
Hazard Analysis. Verify that software modifications correctly implement the critical requirements and introduce no new hazards. Update the hazard analysis.	Proposed Changes Installation Package Hazard Analysis Report	Task Report(s) – Hazard Analysis Anomaly Report	PM, QE, SM, SE
Risk Analysis. Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks.	Installation Package Proposed Changes Hazard Analysis Report Supplier Development Plans and Schedules Operation problem reports V&V task results	Task Report(s) - Risk Analysis Anomaly Report(s)	PM, QE, SM, SE

4.6.1.1 During the maintenance phase, the developers may be assigned to other projects and may not be readily available to assist.

Impact: Lack of resources for immediate response to problems.

Action: Plan that resources familiar with the development be available to complete the maintenance phase work.

5 Software Verification and Validation Reporting

This section describes how the results of implementing the Plan will be documented.

5.1 Task Reporting

A report of each of the Tasks/Sub-tasks performed in the SVVP shall be developed and issued as they are completed. Listed below are the different reports to be generated.

Management	Progress reporting and internal notes
Documentation Evaluation	Documentation checking forms with review reports
Software/Firmware Testing	Software test report
Acceptance Testing	Acceptance Test Report
Others	Meeting reports or internal notes

5.2 V&V Phase Summary Report

A phase Summary Report shall summarize the results of V&V tasks performed in each of the following life-cycle phases: Requirements, Design, Implementation and Test. Each V&V Phase Summary report shall contain the following:

5.2.1 Description of SV&V tasks performed

5.2.2 Summary of test results

5.2.3 Summary of anomalies and resolutions

5.2.4 Recommendations

5.3 Anomaly Report

An anomaly report shall document each anomaly detected in the SV&V. The report content and administrative controls are provided in 7.1

5.4 Final Software Verification and Validation Report

The final report shall include a summary of the V&V activities and results. Deviation from the SV&V plan will be noted. Both positive and negative findings will be reported. Based on the results of the V&V, a conclusion and recommendations for further actions will be provided.

The format of the final report will be as follows:

Summary of each phase, to include:

5.4.1 Task results

5.4.2 Anomalies

5.4.3 Anomaly Resolution

5.4.4 Overall Quality Assessment

5.4.5 Conclusions

5.4.6 Recommendations

6 Verification and Validation Administrative Procedures

6.1 Anomaly Reporting and Resolution

As identified, anomalies will be written, and forwarded to the PM for logging. Each anomaly will be sequentially numbered by the PM.

Each anomaly will be presented to the review team for discussion and resolution. If mutual agreement cannot be reached, the PM will resolve the anomaly, and the process completed. Based on the severity of the anomaly, the originator may stop work, and request an immediate review meeting. Otherwise, the anomaly will be reviewed at the completion of the current V&V task, or phase.

6.2 Task Iteration Policy

A change request regarding a version results in the following processing with respect to the SV&V life cycle:

6.2.1 Analysis of the impact of the change (identification of items involved and the degree of the modification)

6.2.2 Repetition of the V&V cycle on items which change in order to check that the modifications have been taken into account in version n+1

6.3 Deviation Policy

When a deviation to the SVVP is identified, generation of an ECN, as described in QSP-05-08 will be required.

6.4 Control Procedures

All documents produced under the V&V program will be controlled and stored as any other engineering document, as described in QSP-05-08.

SRM classifies firmware as a drawing and therefore, follows SRM QSP-205 and QSP-05-08, Engineering/Document Change Notice Procedure, for its control. To this extent, the problem is documented using the Engineering Change Notice (ECN) procedure and sent to the Project Manager. Upon evaluation, the ECN will: 1) Be approved and implemented; 2) Be forwarded to the appropriate department for further action or; 3) Be returned with an explanation. Upon resolving the problem, the applicable documentation will be revised, and the corrected firmware will be released using the Engineering Change Notice (ECN).

Problems relating to monitor operation must be formally directed to the cognizant project engineer or Project Manager in the form of a field problem report. The format of the field problem report is not critical; however sufficient information (i.e., tag number, description of problem, operating mode, results observed, etc.) must be provided to permit the problem to be reproduced. The project engineer, or manager, will be responsible for resolving the problem report and, if required, initiate an internal ECN (per QSP –05-08) to revise the applicable firmware and documentation as required in this SVVP. Testing of revised firmware will be performed on hardware similar to that originally tested on.

Repetition of the affected portion of the V&V program will be required for and change affecting software that has been formally subjected to a V&V program.

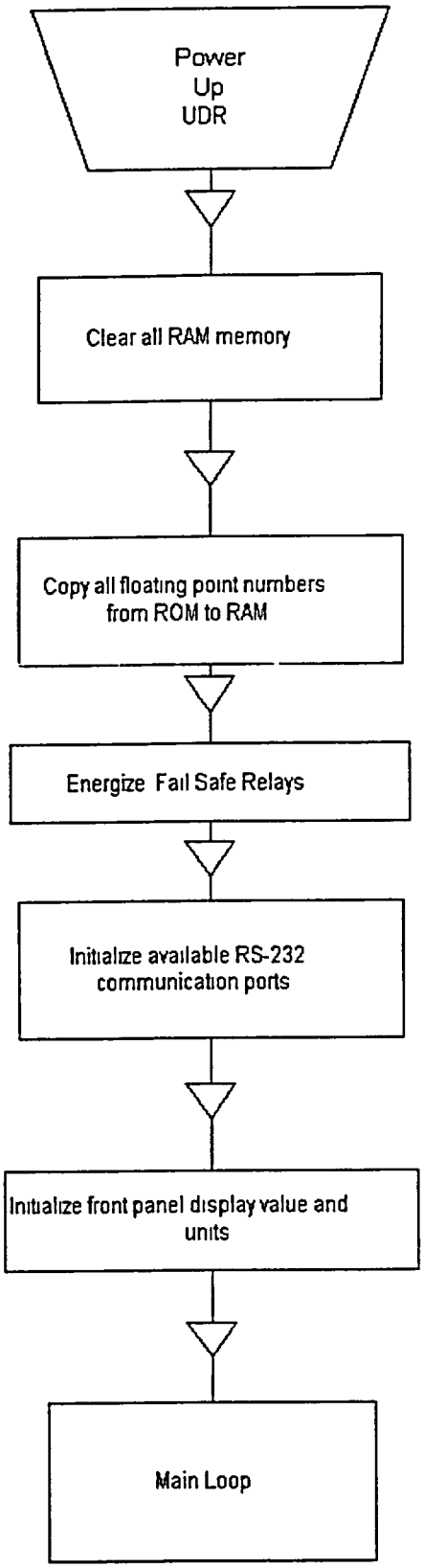
6.5 Standards, Practices, and Conventions

Refer to Section 4.0

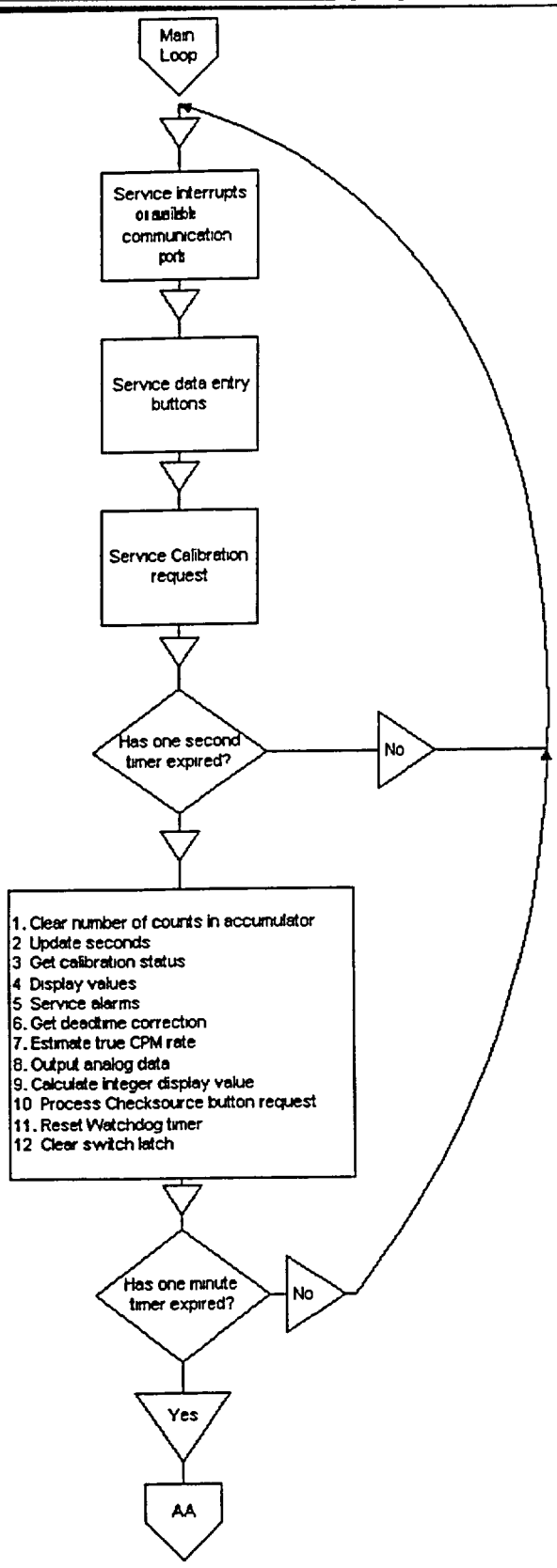
APPENDIX A: List of all documents to be generated under this SVVP

Document Number:	Description:
94095603SDD	Software Design Description
94095603SRS	Software Requirements Specification
94095603VVTP	Verification and Validation Test Procedure
94095603VVTR	Verification and Validation Test Report

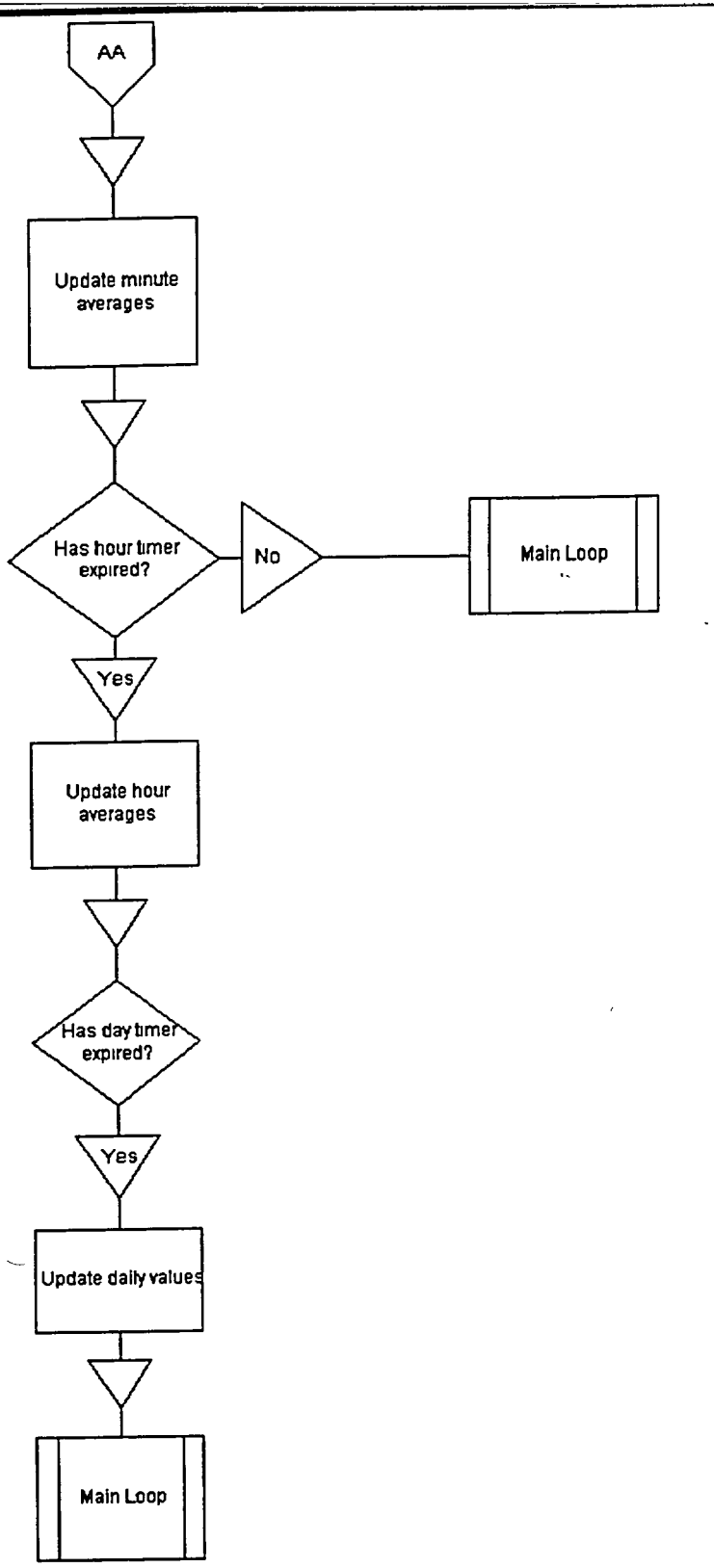
ADDENDUM 1 – Firmware Flowchart, Page 1 of 3 pages



SYNCOR RADIATION MANAGEMENT			DATE 9/11/02		TITLE SOFTWARE VERIFICATION AND VALIDATION PLAN, 94095603	
REV	ECN NO.	RELEASED FOR PRODUCTION	DOC CTRL	SHEET 1 of 3	NO. 94095603VVP	SIZE
1	3044					



SYNCOR RADIATION MANAGEMENT			DATE 9/11/02		TITLE SOFTWARE VERIFICATION AND VALIDATION PLAN, 94095603	
REV	ECN NO.	RELEASED FOR PRODUCTION	DOC CTRL	SHEET 2 of 3	NO. 94095603VVP	SIZE
1	3044					



SYNCOR RADIATION MANAGEMENT			DATE 9/11/02		TITLE SOFTWARE VERIFICATION AND VALIDATION PLAN, 94095603	
REV 1	ECN NO. 3044	RELEASED FOR PRODUCTION	DOC CTRL	SHEET 3 of 3	NO. 94095603VVP	SIZE

Victoreen
Model 94X UDR
Product Information Bulletin

MODEL 94X DIGITAL RATEMETER

PRODUCT INFORMATION BULLETIN

Subject: Firmware Verification and Validation

The Victoreen 94X Series Digital Ratemeters were originally designed in 1984, for the purpose of upgrading the 1960s vintage Analog Ratemeters that were currently being used in the nuclear power industry. Since its introduction, well over 1000 units have been successfully installed and are in operation on a daily basis.

The 94X Series Digital Ratemeter (UDR) is a microprocessor based device, whose operation is controlled by the installed firmware. The basic functions of the Digital Ratemeter are to convert the input pulses from the detector into a digital value, and to compare this value with an operator entered alarm setpoint. When the alarm setpoint is exceeded, a relay, operated in the fail-safe mode, changes state, advising plant personnel that a significant change in radiation level has occurred. The relay contact output may be interlocked with a plant annunciator or a process control interlock.

At the time of the Digital Ratemeter's initial design, formal firmware verification and validation (V & V) requirements were not in widespread use in the industry. Formal V & V documentation, therefore, does not exist for this device. The basic firmware itself, however, has been in use since 1985, and has been an extremely reliable product for Victoreen's customers. We believe the large installed base of UDR radiation monitors is sufficient to justify an exemption to formal V & V documentation. The actual firmware installed in each Digital Ratemeter, including changes, is controlled and verified as follows:

- All firmware/software releases and changes are controlled under Engineering Instruction EI001. This document controls the following items:

  - Final Product Master Set: Media required to produce copies of the firmware/software for shipment.
  - Source Files: Files and data required to reproduce the Final Product Master Set.
  - Software Control Document: Provides information necessary to modify or reproduce the Final Product Master Set. Include information on editors, compilers, development system, assemblers, linkers, etc. used in developing the master set. A revision history summary is now also required.
  - Preparation of a second Final Product Master Set for off-site storage.
  - Part Numbering Format
  - Defines the firmware/software as a document, and imposes generic document review and change control measures.

- All firmware changes are controlled under our generic Document Control Procedure, S.O.P. 410.307. This requires definition of changes and review by Engineering and Quality Assurance.

- All firmware operated products are subjected to a functional test prior to shipment by an independent Test Department.

- All customer specific firmware changes are identified and controlled by the assignment of a unique part number. Specific test procedures are prepared to verify the change requested has been properly implemented.

The firmware in the UDR does not contain a sophisticated operating system. Its operation is a basic clock-controlled loop, repeating once each second. That is, from the main loop program, the firmware jumps to a specific series of program subroutines. In the event the firmware does not complete all of the subroutines (up to 31) and return to the main loop, the hardware "Watchdog" timer will time out, illuminating the FAIL lamp, and de-energizing the FAIL relay.